Command and Control Network Access

A concept presentation
to the CLCS User Liaison Team

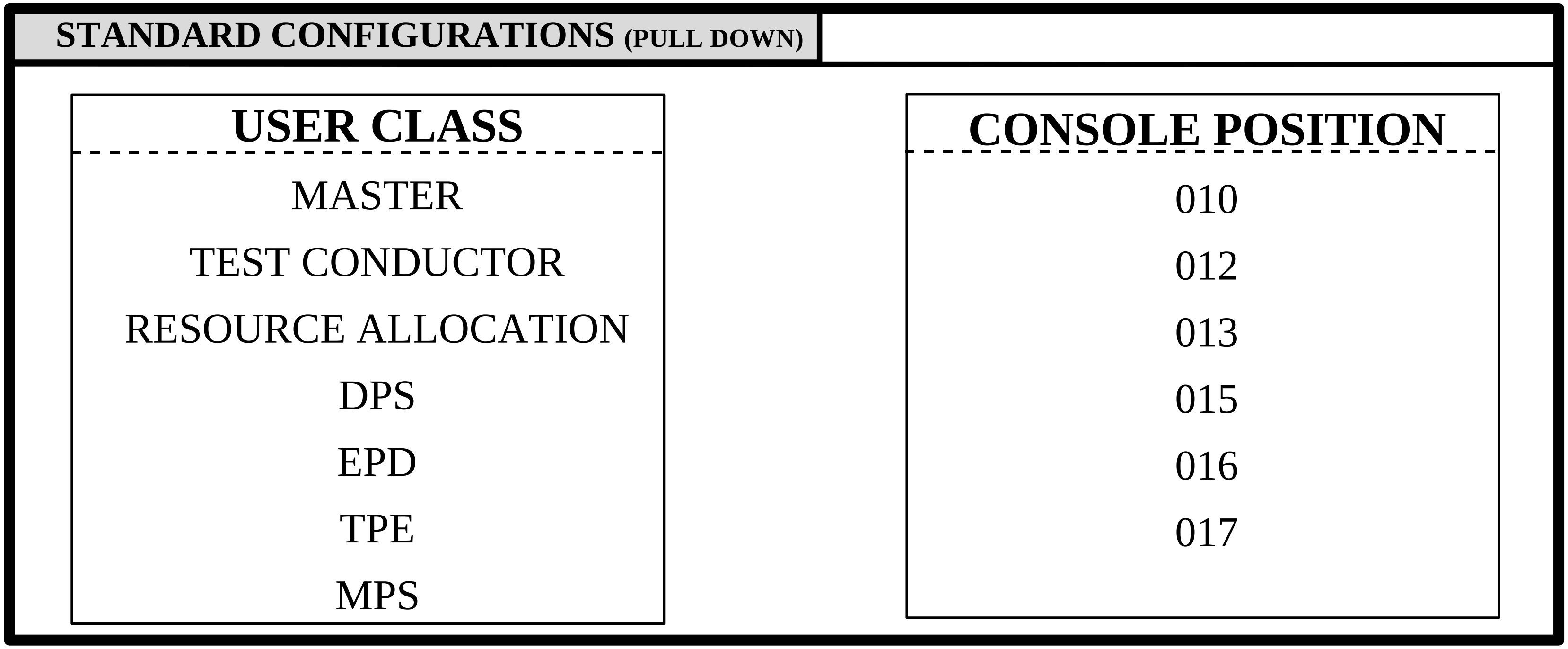
6/10/97

CLCS User Access

- Charter
  - Develop a command and control access methodology for CLCS
- Goals
  - Provide an access control system with inherent flexibility
  - Eliminate problems associated with “RSYS”
  - Allow multiple user classes to “control” the same system
  - Allow one user class to “control” multiple systems
  - Preclude ‘inadvertent’ commanding
  - Allow any user class to view any data
  - Minimize creation of new organizations to manage user accounts
  - Don’t preclude temporary transfer of some user class functions

Concept

- Disassociate person from “command” authority
- Command authority is “mask” at HCI level
- The only user class requiring UID and password is Master



STANDARD CONFIGURATIONS (PULL DOWN)

USER CLASS

MASTER
TEST CONDUCTOR
RESOURCE ALLOCATION
DPS
EPD
TPE
MPS

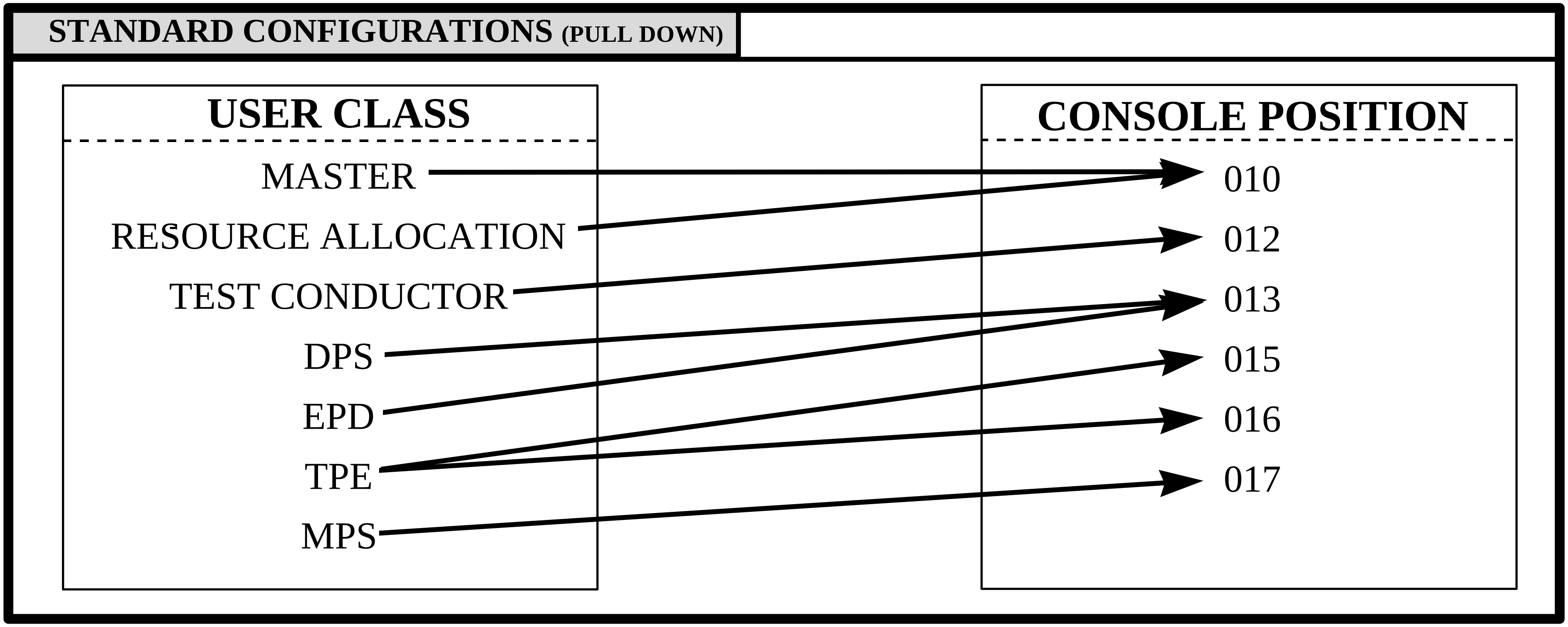
CONSOLE POSITION

010
012
013
015
016
017

Resource Screen Concept

Note: Graphics represented are for informational (notional) purposes only
Actual screen layouts to be worked later

Resource allocation example



STANDARD CONFIGURATIONS (PULL DOWN)

USER CLASS

MASTER
RESOURCE ALLOCATION
TEST CONDUCTOR
DPS
EPD
TPE
MPS

CONSOLE POSITION

010
012
013
015
016
017

Example:
- Master located at position 010 (with resource allocation authority)
- TC active at console position 012
- Console position 013 has DPS and EPD command authority
- TPE located at two positions (015, 016)
- MPS assigned one workstation (017)

Note: Graphics represented are for informational (notional) purposes only
Actual screen layouts to be worked later

The Process

- Master logs on and configures equipment (CCP, DDP, gateways)
- User enters OCR (or remote/local control area)
- User checks in with TC*
- TC directs User to desired console position
- User reports “on-net”
- TC communicates with Master to place User Class at console position
- User ‘pulls down’ standard menu and selects desired command system
    - User can monitor ANY system
    - User has command authority ONLY for requested system(s)
    - User can query for command assignment
    - Command authority verifiable on screen
- User can request reallocation command authority at any time
    - Can acquire more capability
    - Can relinquish no longer needed capability
- Non allocated, available console positions are active in monitor only mode

*note: TC checks in with Master when set is inactive

-

Notes

- User group is lowest level of independence
  - No requirement for ‘unique’ user files/capabilities (User accesses group files only)
  - System look and feel is consistent for all members of the group
- No requirement for unique User ID/Password*
  - Issue needs to be worked
  - Waiver available for FIPS (Federal Information Processing Standard) requirement
  - No requirement to associate individual User with commandability
  - Existing User discipline enforced

*Master requires UID and password to configure system resources (i.e, root)

Summary

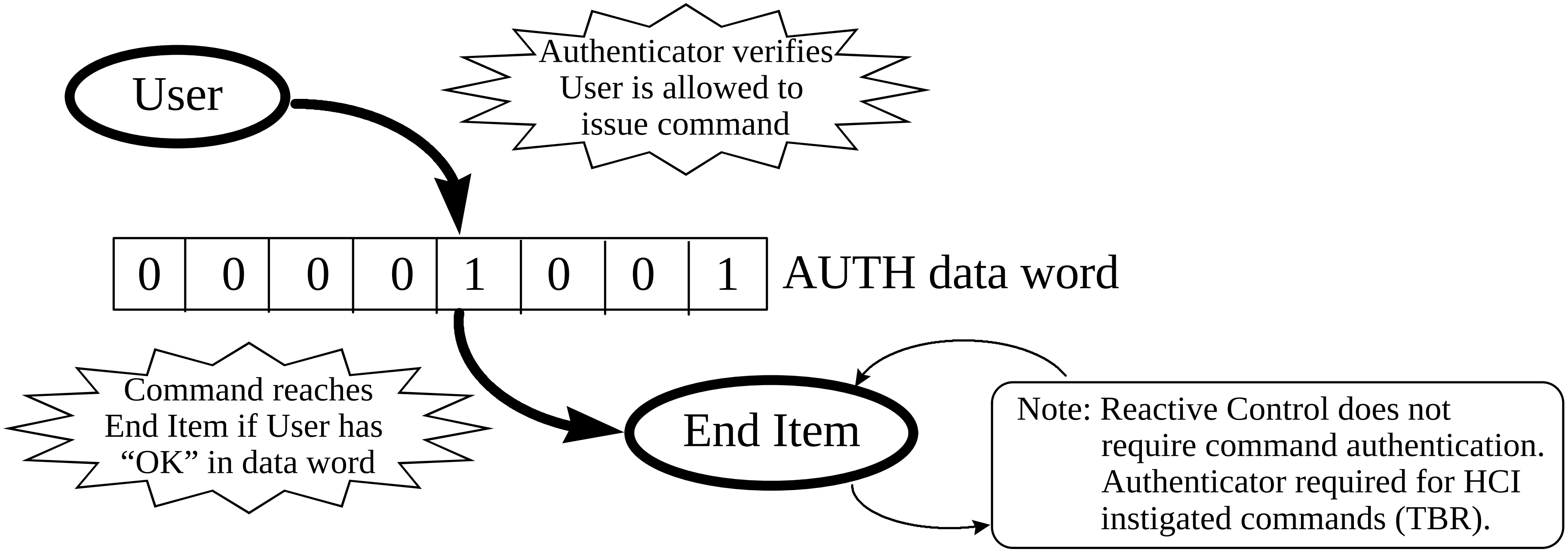
- Advantages
  - System is very flexible
    - Command reassignment can be automated for critical operations
      - No loss of controllability
      - Eliminates emergency safing should a console position fail
    - System supports multiple user classes at same console
    - System supports the same class at multiple consoles
  - Standard layouts can be predefined
  - Reconfiguration after failure is quick
  - Multi-flow (cross OCR) capabilities are possible
  - Proposed User access is more capable than CCMS or baselined CLCS

- Action
  - Present concept to CLCS Program Management for adoption (SLS change)

Command “Authentication”

backup page

- Command RSYS needs investigation
  - Implementation could use data word reserved for user class
  - Multiple commanders possible (if desired)
  - Not limited to “systems”, includes Set Support, O&M, TPE and others
  - Command authenticator verifies command issuer has match in data word
  - Functionality needs further research (will be forwarded to SAT)


User
Authenticator verifies User is allowed to issue command
Command reaches End Item if User has “OK” in data word
End Item

0	0	0	0	1	0	0	1	AUTH data word

Note: Reactive Control does not require command authentication. Authenticator required for HCI instigated commands (TBR).

Data presented on this page is conceptual and is subject to revision.
It does not imply a final implementation